WILSHIRE LAW FIRM
BOBBY SAADIAN, Esq. SBN: 250377
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Tel: (213) 381-9988
Fax: (213) 381-9989

GIRARDI | KEESE
THOMAS V. GIRARDI, State Bar No. 36603
tgirardi@girardikeese.com
SAMANTHA GOLD, State Bar No. 314048
sgold@girardikeese.com
1126 Wilshire Boulevard
Los Angeles, California 90017
Telephone: (213) 977-0211
Facsimile: (213) 481-1554

Attorneys for Plaintiffs and Proposed Class

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION – LOS ANGELES

STEVEN J. BRETT; AMERICA MUNSON; SCOTT ABLES, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

BROOKS BROTHERS GROUP, INC., a Delaware corporation,

Defendant.

CASE NO.: 2:17-cv-04309-DMG-E

SECOND AMENDED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs, America Munson, Steven J. Brett, and Scott Ables ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action based upon personal knowledge as to themselves and their own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigations of their attorneys.

I. NATURE OF THE ACTION

1. Tens of thousands of customers every year shop at Brooks Brothers Group, Inc. (hereafter as either "Brooks Brothers" or "Defendant"), known for their high-quality suits. Consumers expect the highest quality merchandise and services from Brooks Brothers. What consumers did not expect was that at 223 store locations, for a period of 11 months, customers' information was being collected by an unauthorized third party.

2. Plaintiffs, individually and on behalf of those similarly situated persons (hereafter "Class Members"), bring this class action based on California law to secure redress for Brooks Brothers' reckless and negligent violations of its customers' privacy rights. Plaintiffs and Class Members are former Brooks Brothers customers who shopped at some of their 223 stores in the U.S. and Puerto Rico during the period of April 4, 2016 to March 1, 2017.

3. Plaintiffs and Class Members suffered injuries as a result of a security breach compromising Brooks Brothers store customers' names, credit and debit card account numbers, card expiration dates, and card verification codes, which included Personal Identifiable Information, in addition to other private information as described below ("PII").[1]

[1] Cal. Civ. Code § 1798.81 defines Personal Information to mean the following:
(A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
(i) Social security number.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

4. As a result of Defendant's wrongful actions and inactions, customer information was stolen from Brooks Brothers' point-of-sale ("POS") network. Many of Defendant's customers had their Personal Identifiable Information compromised, their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages.

II. THE PARTIES

5. Plaintiff Scott Ables ("Plaintiff Ables") is a California citizen residing in Los Angeles, California. Plaintiff has been shopping at Brooks Brothers for years, and during and after the breach, Plaintiff had several fraudulent charges to credit and debit cards used at Brooks Brothers' stores. Moreover, Plaintiff had to spend time and effort to cancel every debit and credit card used at Brooks Brothers' stores, and Plaintiff had and still has to constantly monitor his accounts due to the risk of fraud and identity theft. Plaintiff Ables has never knowingly been victimized by a data breach other than the one subject to this action. Plaintiff Ables closely monitors his bank account, regularly checking it online at least every other day for irregular activity. He regularly shreds his hard copy credit card and financial account statements.

6. Plaintiff America Munson ("Plaintiff Munson") is a California citizen residing in Vallejo, California. Plaintiff Munson has been a customer of Defendant since 2010 and made purchases with her credit and debit cards during that time. At all relevant times hereto, Plaintiff Munson shopped at the following

---

(ii) Driver's license number or California identification card number.
(iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(iv) Medical information.
(v) Health insurance information.
(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Brooks Brother's locations in California: Napa, San Francisco, and San Mateo. Plaintiff has provided her PII to Defendant at all times that she has made a purchase with Defendant. Shortly after the breach, Plaintiff's debit and credit card information was accessed by hackers. Plaintiff Munson has never been victimized by a data breach other than Brooks Brothers'. Plaintiff Munson has used her Brooks Brothers credit card and at least two different debit cards for different purchases with Defendant for a number of times during the timeframe of the data breach. One of the at least two debit cards that Plaintiff Munson used to make purchases at Defendant's stores had to be cancelled due to Plaintiff Munson finding fraudulent activity in her account. In addition, Plaintiff has to purchase credit and personal identity monitoring service to alert her to potential misappropriation of her identity and to combat the risk of further identity theft. Exposure of Plaintiff's identifying personal information has placed her at imminent, immediate and continuing risk of further identity theft-related harm. Plaintiff Munson also suffered from the deprivation of the value of her PII and the lost benefit of the bargain.

7. Plaintiff Steven J. Brett ("Plaintiff Brett") is a California citizen residing in Cabazon, California. Plaintiff is a long-time customer of Defendant, who has shopped a number of times at Defendant's physical stores, including before, during, and after the alleged timeframe of the data breach. Plaintiff has provided his personal identifying information to Defendant at all times that he has made a purchase. Shortly after the breach, Plaintiff's debit and credit card information was accessed by hackers. In addition, Plaintiff has to purchase credit and personal identity monitoring services to alert him to potential misappropriation of his identity and to combat risk of further identity theft. Exposure of Plaintiff's identifying personal information has placed him at imminent, immediate and continuing risk of further identity theft-related harm. Plaintiff Brett also suffered from the deprivation of the value of his PII and the lost benefit of the bargain.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

8. Plaintiffs bring this action on their own behalf and on behalf of all others similarly situated; namely, all individuals who have made a purchase at any of Brooks Brothers' 223 stores during the period of April 4, 2016 to March 1, 2017. Plaintiffs' and Class Members' PII is currently being sold on the black market.

9. Defendant Brooks Brothers is a Delaware corporation with its principal place of business in New York, New York. Brooks Brothers has registered with the California Secretary of State to be served for any action filed against it in California through its agent for service of process: Corporation Service Company, 2710 Gateway Oaks Dr., Ste 150N, Sacramento, California, 95833.

III. JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over the state law claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since some of the Class Members are citizens of a State different from the Defendant and, upon the original filing of this complaint, members of the putative Plaintiff class resided in states around the country; there are more than 100 putative class members; and the amount in controversy exceeds $5 million.

11. The Court also has personal jurisdiction over the parties because, on information and belief, Defendant conducts a major part of its national operations with regular and continuous business activity in California through a number of stores and with an advertising budget not exceeded in other jurisdictions throughout the United States.

12. Venue is appropriate in this District because, among other things: (a) Plaintiffs are residents of this District and citizens of this state; (b) Defendant directed its activities at residents in this District; and (c) many of the acts and omissions that give rise to this Action took place in this judicial District.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

13. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because Defendant conducts a large amount of its business in this District, and because Defendant has substantial relationships in this District.

IV. SUBSTANTIVE ALLEGATIONS

A. Brooks Brothers' Point-of-Sale System

14. Retail Brand Alliance Inc. ("RBA") purchased Brooks Brothers in 2001. Following its purchase, in 2002 RBA replaced the Retek Merchandising Solution with JDA Portfolio(R) merchandise management software to manage the operations of Brooks Brothers.[2,3] RBA emphasized the goal of having Brooks Brothers' customers' information interconnected throughout all of its stores. Stefano Gaggion, the vice president of Management Information System at RBA, emphasized this goal by stating: "One Tool, One Way, One Solution . . ." which would allow for "volumes of customer information," across stores.[4]

15. Furthermore, on July 1, 2002, Denise Albright, VP of planning and allocation for RBA, stated, "[w]e always have data integrity and constant reporting across the company in one common, easy to use format."[5] On August 1, 2003, Brooks Brothers announced going live with JDA Softwares.[6] Stefano Gaggion, now Chief Information Officer ("CIO") of RBA, participated in a technology round-table discussion on maintaining customer relationships and RBA's choice of an all-Java enterprise application for POS: [7]

---

[2] *Brooks Brothers Goes Live with JDA Software*, available at: https://www.thefreelibrary.com/Brooks+Brothers+Goes+Live+with+JDA+Software%3B+JDA+Portfolio+Provides...-a091383603 (attached hereto as **Exhibit A**).

[3] All cited websites were last visited on June 14, 2018.

[4] *Id*.

[5] *Retail for All Seasons*, available at: https://risnews.com/retail-all-seasons (attached hereto as **Exhibit B**).

[6] **Ex. A**.

[7] *Retail's IT Pacesetters*, available at: https://risnews.com/retails-it-pacesetters (attached hereto as **Exhibit C**).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

> Last year RBA selected an all-Java enterprise application for POS from ADS Retail. Gaggion says the company will grow its business "by utilizing multi-channels, which integrate information between retail locations, direct marketing and wholesale customers. Key information will be shared via a Web-browser solution." He adds that data, "such as demographics, product preferences and size tendencies will be gathered about the customers and shared with our partners, stores and wholesale customers to drive sales and profitability.

16. Indeed, Brooks Brothers' utilized a Java based solution, NEXTOR I POS, with the goal of linking all of their brand stores together as one unit.[8]

17. In 2007, Brooks Brothers switched POS systems and implemented a Java based "clienteling" system that monitors customer behavior, including POS data: "[t]he system records all interactions salespeople have with customers. It reminds associates to correspond with shoppers regarding special offers, birthdays and other information. . . [t]he product also keeps track of alterations and customer preferences." [9]

18. Payment Card Industry Data Security Standard ("PCI") sets the standard for security practices in relation to POS. As early as 2008, Stefano Gaggion, SVP & CIO of Brooks Brothers, criticized the PCI compliance. He explained that PCI compliance should be done by credit card companies, and not retailers:[10]

> The challenge is made more difficult by the lack of clear direction and requirements. Since no one is taking responsibility for owning PCI, each retailer struggles with

---

[8] *Retail Brand Alliance, Inc. Selects Nextor Point-of-Sale Application For Its 1,000+ Stores*, available at: https://www.digitalcommerce360.com/2003/01/02/retail-brand-alliance-inc-selects-nextor-point-of-sale-appl/ (attached hereto as **Exhibit D**).

[9] *Brand Empowerment*, available at: https://risnews.com/brand-empowerment (attached hereto as **Exhibit E**).

[10] *What Keeps CIOs Up At Night*, available at: https://risnews.com/what-keeps-cios-night (attached hereto as **Exhibit F**).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

> the challenges rather than working through a common, standard set of repeatable regulations. The lack of partnership makes the process adversarial. Since the credit card companies already have all the customer data (including authorizations) in their databases, they should own the authorization information. Then, they would be able to protect the customer and guarantee the safety of the data.

19. In 2009, Visa issued a Data Security Alert (which Brooks Brothers should have reasonably been aware of) outlining the threat of RAM scraper malware.[11] The report instructs companies to "[s]ecure remote access connectivity," "[i]mplement a secure network configuration, including egress and ingress filtering to only allow the ports/services necessary to conduct business" (i.e., segregate networks), "actively monitor logs of network components, including IDS [intrusion detection systems] and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses," "[e]ncrypt cardholder data anywhere it is being stored and [] implement[] a data field encryption solution to directly address cardholder data in transit" and "[w]ork with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration."[12]

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

[11] *Visa Data Security Bulletin*, 2009, available at: http://visa.com.ph/ap/sg/merchants/include/improper_seg_network.pdf (attached hereto as **Exhibit G**).

[12] *Id.*

20. By March 2015, credit card companies set an October deadline for companied to switch to chip-enables cards installed in POS systems. Brooks Brothers' CEO, Claudio Del Vecchio was displeased with paying for upgrades.[13,14]

21. All merchants that accept customer payments via payment cards, including Brooks Brothers, are and were required to comply with the Payment Card Industry Data Security Standards (the "PCI DSS").[15] As stated, "if you are a merchant that accepts payment cards, you are required to be complaint with the PCI [DSS]." Compliance with the PCI DSS is common practice in the retail industry. The PCI DSS, among other things, mandates merchants to protect cardholder data,[16] which requires merchants to install and maintain firewalls,[17] forbids merchants from using default settings and passwords for applications and devices,[18] requires merchants to segment cardholder data,[19] and requires merchants to identify and authenticate their system users.[20]

22. Additionally, sub-requirement 3.2 of the PCI DSS requires merchants and other organizations involved in payment card transactions to **refrain from**

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

[13] *Costly Shift To New Credit Cards Won't Fix Security Issues*, available at: https://www.reuters.com/article/us-usa-cybersecurity-retail-insight/costly-shift-to-new-credit-cards-wont-fix-security-issues-idUSKBN0LZ0GC20150303 (attached hereto as **Exhibit H**).

[14] *Retailers face $8.65 billion bill for new generation of credit cards*, available at: http://fortune.com/2015/03/03/retailers-face-8-65-billion-bill-for-new-generation-of-credit-cards/ (attached hereto as **Exhibit I**).

[15] *How to Be Compliant: Getting Started with PCI Data Security Standard Compliance*, PCI SSC, *available at* https://www.pcisecuritystandards.org/merchants/how_to_be_compliant.php (attached hereto as **Exhibit J**).

[16] *Id.* at 34.

[17] *Id.* at 19.

[18] *Id.* at 28.

[19] *Id.* at 61.

[20] *Id.* at 64.

storing sensitive authentication data after authorization (even if it is encrypted).[21] To adhere to the PCI DSS, a merchant must, *inter alia*:

> First, **Assess** -- identify cardholder data, take an inventory of your ITassets and business processes for payment card processing, and analyze them for vulnerabilities that could expose cardholder data. Second, **Remediate** -- fix vulnerabilities and do not store cardholder data unless you need it. Third, **Report** -- compile and submit required remediation validation records (if applicable), and submit compliance reports to the acquiring bank and card brands you do business with.[22] [emphasis on the original].

23. As of December 2016, Brooks Brothers was not PCI compliant. It signed a contract with SkillNet Solutions to implement the Oracle Retail Xstore POS system.[23] "After an intensive review of the Oracle partners in the field, we selected SkillNet's Professional Services and Expert Services teams to support and enhance our store systems," said Sahal Laher, EVP and CIO of Brooks Brothers.[24]

24. Around the time of the Brooks Brothers' data breach subject to this action, Zach Paul, Brooks Brothers' Payment and Retail Systems Analyst, "[w]orked to roll out EMV and NFC technologies to the **Verifone Pinpads**." [emphasis added][25] The Verifone Pinpads operates on Windows XP. EMV is the standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions. NFC is a technology standard that essentially uses radio signals for two-way communication at very small range. Debit and

---

[21] *See id.* at 35.
[22] *Id.*
[23] *Brooks Brothers Selects SkillNet Solutions Retail Suite*, available at: https://www.retailtouchpoints.com/features/news-briefs/brooks-brothers-selects-skillnet-solutions-retail-suite (attached hereto as **Exhibit K**).
[24] *Id.*
[25] *Linkedin of Zach Paul*, available at: https://www.linkedin.com/in/zpaul (attached hereto as **Exhibit L**).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

credit cards have EMV embedded chips and antennae that enable contactless capabilities just like NFC-enabled devices.

B. The Malware

25. On May 10, 2018, hackers leaked a complete source code for malware affecting major retailers across the country was leaked online . The malware known as TreasureHunter (also known as TreasureHunt) was created by the Bearsinc computer crime syndicate, a dangerous criminal organization notorious for mass identity theft and credit card fraud.[26]

26. TreasureHunter malware targets retail POS systems with weak security credentials by embedding a tiny file in a large directory where the malware persistently collects data over time and transmits it to a server outside the United States.

27. However, upon information and belief, evidence regarding the POS malware identified as "TreasureHunter" and its potential threat to such POS systems was published by various organizations as early as March 2016. The published information describes the threat of POS malware as a type of malicious software that extracts payment card information from memory and usually uploads that data to a command and control server.[27] "Although the PCI DSS rules changed in October 2015, leaving retailers who have not transitioned from existing 'swipe' cards to EMV or 'chip' enabled cards liable for card present fraud in more ways than before, many retailers are still in the process of transitioning to chip-enabled card technology. Criminals appear to be racing to

[26] *Author of TreasureHunter PoS Malware Releases Its Source Code*, available at: https://www.darkreading.com/vulnerabilities---threats/author-of-treasurehunter-pos-malware-releases-its-source-code-/d/d-id/1331778 (attached hereto as **Exhibit M**).

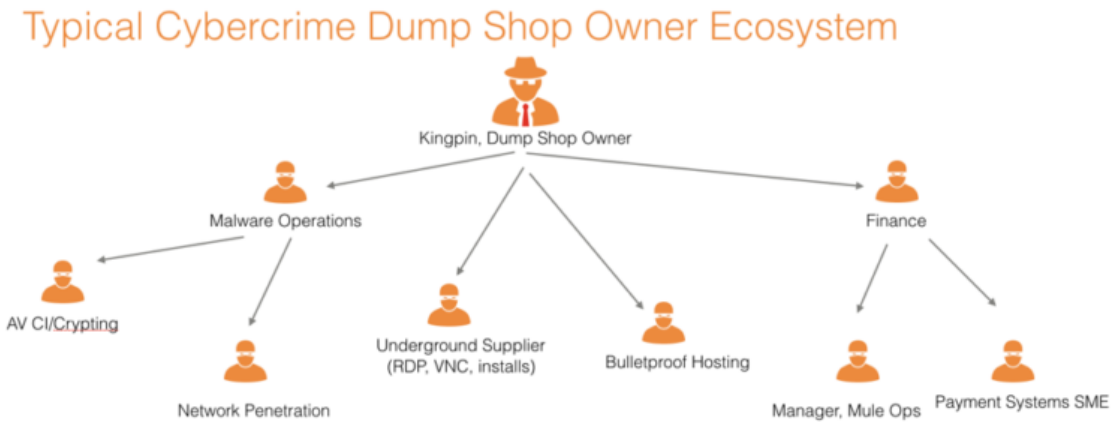
[27] *TREASUREHUNT: A Custom POS Malware Tool*, available at: https://www.fireeye.com/blog/threat-research/2016/03/treasurehunt_a_cust.html (attached hereto as **Exhibit N**).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

infect POS systems in the United States before US retailers complete this transition."

28. TreasureHunter attacks unpatched Windows XP based systems, and targets POS systems not yet converted to EMV technology, including the Verifone Pinpads utilized by Brooks Brothers.

29. The Bearsinc crime syndicate uses "command and control" servers to consolidate large blocks of consumer data from compromised retailers. This is known as a "dump shop." The packaged data is sold in bulk on the black market to lower tier identity theft criminals in exchange for untraceable bitcoin or other cryptocurrencies.



30. TreasureHunter behaves like many other point-of-sale malwares. Once an attacker has access to a Windows-based server and the POS terminal, the malware is installed, and it establishes persistence by creating a registry key that runs the malware at startup. It then enumerates running processes and scans device memory looking for track data, including primary account numbers, separators, service codes, and more. It then establishes a connection with the attacker's command and control server and sends the stolen data to the criminal.[28]

[28] *TreasureHunter Point-of-Sale Malware and Builder Source Code Leaked*, available at: https://www.flashpoint-intel.com/blog/treasurehunter-source-code-leaked/ (attached hereto as **Exhibit O**).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

31. On or before 2016, the malware TreasureHunter affected Brooks Brothers' POS systems, which affected virtually all of Brooks Brothers' stores.[29]

C. The Brooks Brothers' Data Breach Unravels

32. According to the Defendant, on or about April 4, 2016, the malware was installed at POS systems at Brooks Brothers' stores. This affected 223 Brooks Brothers' locations disclosed by Defendant. The malware siphoned off customers' full names, card account numbers, expiration dates, and verification codes. In addition, however, based upon information and belief, hackers were also able to acquire stores' zip codes and locations linked to purchases, and time of the transactions.

33. With the information acquired, additional derivative information can be obtained. When this additional and otherwise innocuous information, such as the other aforementioned disclosed data, is combined with debit/credit card information, that permits a hacker to easily commit identity theft and identity fraud.[30]

34. Until around March 1, 2017, the Malware kept acquiring customers' PII from the 223 Brooks Brothers' store locations. Defendant had previously set a website which alerted customers on which stores were affected, named "Incident locations" at www.brooksbrothers.com/incident-locations. Defendant has now removed any notice of the data breach.

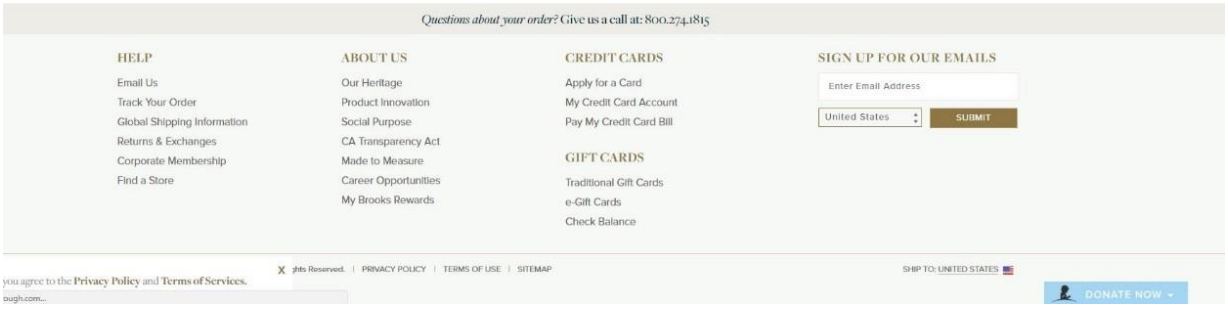
[29] Alternatively, the top POS malwares are the following: Nitlove PoS; PoSeidon; MalumPOS; CherryPicker; AbaddonPOS. Available at: https://duo.com/blog/a-breakdown-of-different-types-of-point-of-sale-malware (attached hereto as **Exhibit P**).

[30] Hackers are easily able to acquire additional information such as date of birth, current and past addresses, phone numbers, e-mail addresses, driving records, criminal records, and possible relatives, with a simple public record search that requires not more than an individual's full name. *See New Website Exposes Driving Histories*, available at: http://www.wnd.com/2018/06/new-website-exposes-driving-histories/ (attached hereto as **Exhibit Q**).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

35. It was not until May 12, 2017, over thirteen (13) months after the data breach began, Brooks Brothers disclosed this breach on its website.[31,32] On May 12, 2017, Brooks Brothers admitted that the security breach included "name, payment card account number, card expiration date, and card verification code." *Id*. In addition, however, based upon information and belief, hackers were also able to acquire store zip code and location linked to purchases, and time of the transactions, and potentially much more.[33]

36. However, this disclosure was not prominently placed on Brooks Brothers' website. Rather, Brooks Brothers inserted a small tab in the bottom left corner of the webpage titled "Data Incident." This small tab that then would link the visitor to a separate page, which was only visible if the viewer scrolls to the very end of the webpage. This disclosure is no longer shown on its website:



[*This portion of the page has intentionally been left blank*]

---

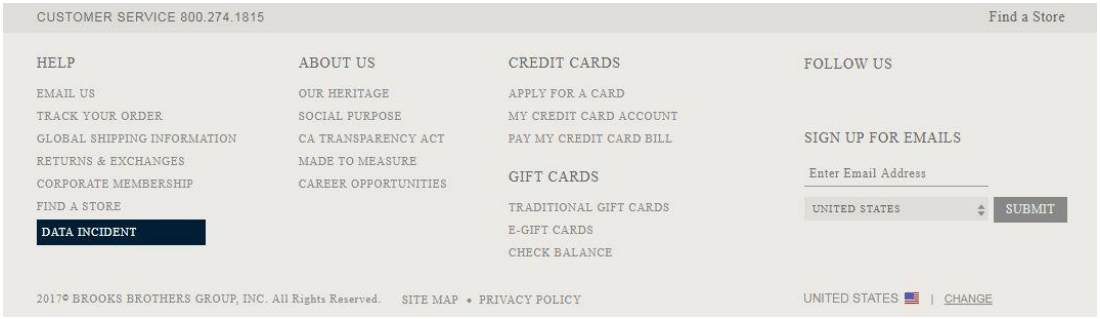
[31] *Brooks Brothers Incident Message*, available at: http://www.brooksbrothers.com/data-incident/incident,default,pg.html (attached hereto as **Exhibit R**).

[32] *Brooks Brothers Breach Advisory statement*, available at: https://oag.ca.gov/system/files/Sample%20Notice_9.pdf? (attached hereto as **Exhibit S**).

[33] "[Data] such as demographics, product preferences and size tendencies will be gathered about the customers and shared with our partners, stores and wholesale customers to drive sales and profitability." **Ex. C**.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

37. The old notice on the website appeared at the very bottom of the webpage as shown below:[34]



38. As noted by Brooks Brothers' own privacy policy in effect during the time of the data breach, Brooks Brothers collected customers' information and customers' behavior for its own benefit:[35]

> **Information Collected**
>
> Brooks Brothers values its customers and respects their privacy. We collect customer information in an effort to improve your shopping experience and to communicate with you about our products, services, contests, and promotions. Brooks Brothers recognizes that it must maintain and use customer information responsibly.
>
> We collect information (such as your name, email address, mailing address, and phone and credit card numbers) that you provide when you place an order, join our mailing list, register with us or participate in a contest, promotion or survey. We also maintain a record of your product interests and your purchases online and in our stores.
>
> To serve you better, the information you supply to us is added to our customer database. We will add you to our mailing list. From time to time, you may receive periodic mailings or emails from us about new products and services, discounts, special promotions or upcoming events. If you do not want to receive such emails or mailings from us, please contact us via email, phone, fax or mail (our numbers and addresses are listed below). You may unsubscribe from our email list directly on the website. Telephone numbers are only used to contact you regarding an order placed with Brooks Brothers. They are not used for any promotional purpose(s).
>
> We may combine information you give us online and in our stores as well as information about your product interests and purchases. In addition, we may combine information you provide with demographic information that is publicly available. We use this combined information to enhance and personalize your shopping experience with us, and to communicate with you by email or postal mail about our products, services, contests and promotions that may be of interest to you.

[*This portion of the page has intentionally been left blank*]

[34] *Brooks Brothers' website from May 15, 2017*; Brooks Brothers' Website from June 18, 2018 (attached hereto as **Exhibit T**).

[35] *Brooks Brothers' Privacy Policy from February 20, 2017* (attached hereto as **Exhibit U**).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

39. Today, Brooks Brothers makes it even more clear that the collection of customer information is conducted in an effort to maximize their marketing and "shopping experience," as noted below:[36]

> Information Collected
>
> We collect customer information in an effort to improve your shopping experience and to communicate with you about our products, services, contests, and promotions. Brooks Brothers recognizes that it must maintain and use customer information responsibly.
>
> We collect information (such as your name, email address, mailing address, and phone and credit card numbers) that you provide when you place an order, join our mailing list, register with us or participate in a contest, promotion or survey. We also maintain a record of your product interests and your purchases online and in our stores.
>
> To serve you better, the information you supply to us is added to our customer database. This information is used to communicate with you about new products and services, discounts, special promotions or upcoming events. To modify your communication preferences, please contact us via any of the methods listed below.
>
> Please note that telephone numbers are only used to contact you regarding an order placed with us. They are not used for any promotional purpose(s).
>
> We may combine information you give us online and in our stores as well as information about your product interests and purchases. In addition, we may combine information you provide with demographic information that is publicly available. We use this combined information to enhance and personalize your shopping experience with us, and to communicate with you by email or postal mail about our products, services, contests and promotions that may be of interest to you.

40. The Federal Trade Commission ("FTC") has issued numerous guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[37]

41. In 2016, the Federal Trade Commission ("FTC") updated its publication, *Protecting Personal Information: A Guide for Business*, which establishes guidelines for fundamental data security principles and practices for businesses. The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion

[36] *Brooks Brothers' Current Privacy Policy* (attached hereto as **Exhibit V**).

[37] *Start With Security*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (attached hereto as **Exhibit W**).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

42. The FTC recommends that companies do not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures. network; and verify that third-party service providers have implemented reasonable security measures.[38]

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. In this case, Defendant was at all times fully aware of its obligation to protect the PII of its customers because of its participation in payment card processing networks. Defendant was also aware of the significant repercussions if it failed to do so because it collected payment card data from thousands of customers daily at its stores; Defendant knew that this data, if hacked, would result in injury to consumers, including Plaintiffs and Class members.

[38] *Id.*

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

45. Defendant's apparent knowledge of its duty of keeping information private is shown and supported by Defendant's Privacy Policy in effect during the time of the breach:[39]

> Privacy
> We respect your privacy and, therefore, Brooks Brothers does not sell or rent the personal information you provide to us to any third party you do not wish us to do so. Upon your request, we will not share your personal information with any unaffiliated third party. We may make our mailing list available to carefully screened companies whose products and services might interest you. If you do not wish to receive such mailings, or for us to share your information with any third parties as described above, please contact us via email, phone, fax or mail (below). Include your name and address as it was supplied to us, and indicate "Do Not Share".
>
> Brooks Brothers may share information with its subsidiaries and other affiliated companies, and with other carefully selected vendors and business partners with whom we work. This includes companies that perform fraud prevention/detection services; assist us in providing our products and services to you; assist in maintaining and managing customer information to provide customer and internet services; take and fulfill orders; conduct Brooks Brothers promotions and surveys; or assist us in more effectively communicating with our customers. All companies that act on our behalf are contractually obligated to keep all information confidential and to use the customer information only to provide the services we ask them to perform for you and us. We may provide aggregate statistics about our customers, sales, traffic patterns and related site information to reputable third party vendors. We may disclose Personal Information we collect from you if required to do so by law or in the good-faith belief that disclosure is necessary (a) to obey the law or comply with legal process served on us or our affiliates; (b) to protect and defend our rights or property or the rights or property of other users of our Site; or (c) to act in an emergency to protect the personal safety of users of our Site or the public. . If you register with us to receive promotional emails or postal mailings, you agree that Brooks Brothers may transfer your information to its international Brooks Brothers affiliates who may send you communications directly, depending on your location.
>
> Additionally we may disclose your personal information to the buyer as a result of the sale of stock or substantially all of the assets of Brooks Brothers, whether by merger, acquisition, or similar or related transactions or in the event of a liquidation of the assets of the company.

D. Stolen Information Is Valuable to Hackers and Thieves

46. It is well known, and the subject of many media reports, that payment card data is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto is well known. Despite well-publicized litigation and frequent public announcements of data breaches by retailers, Brooks Brothers opted to maintain an insufficient and inadequate system to protect the PII of Plaintiffs and Class Members.

47. Legitimate organizations and the criminal underground recognize the value of payment information. Otherwise, they would not aggressively seek or pay for it.

48. Credit or debit card information is highly valuable to hackers. Credit and debit card information that is stolen from the POS is known as "dumps."[40] Credit and debit card dumps can be sold in the cybercrime

[39] **Ex. U**.

[40] *Krebs on Security April 16, 2016, Blog Post*, available at: https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cv (attached hereto as **Exhibit X**).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

underground for a retail value of about "$20 apiece." *Id.* Furthermore, this information can also be used to clone a debit or credit card. *Id.*

49. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

E. The Data Breach Has and Will Result in Additional Identity Theft and Identity Fraud

50. Brooks Brothers failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.

51. The ramifications of failing to keep Plaintiffs and Class Members' data secure are severe.

52. Plaintiffs' and Class Members' information accessed in the Brooks Brothers' breach can be used to commit further identity theft by placing Plaintiffs and Class Members at a higher risk of phishing and pharming where hackers exploit information they already obtained to get even more PII.

53. Congress has treated credit card numbers as sufficiently sensitive to warrant legislation prohibiting merchants from printing such numbers on receipts—specifically to reduce the risk of identity theft. *See* 15 U.S.C. § 1681c(g) (2012).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

54. Defendant acknowledges that the stolen information gave hackers the means to commit fraud or identity theft, as Defendant recommended: "we recommend that customers review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. **We urge customers to remain vigilant and continue to monitor statements for unusual activity going forward**."[41]

55. A person whose PII has been obtained and compromised may not see the full extent of identity theft or fraud for years. It may take some time for the victim to become aware of the theft. In addition, a victim may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again on a victim's account.

56. "Phishing" is a form of online identity theft that lures consumers into divulging their personal financial information to fraudulent websites, also known as spoofed websites. For example, a phisher sends an email message to an unsuspecting victim instructing him or her to click on the link to a bank's website (provided in the email) to confirm the consumer's account information. Unbeknownst to the consumer, the website is a convincing fake or copy of the authentic website. The unsuspecting consumer takes the bait and provides the information, thereby enabling the phisher to steal the consumer's personal financial information. The phisher can then use the stolen information to clean out the victim's bank accounts or commit other forms of identity theft.

57. "Pharming" is similar to phishing, albeit more sophisticated. Pharmers also send emails. A consumer compromises his or her personal financial information simply by opening a pharmer's email. The pharming email contains a virus (or Trojan horse) that installs a small software program on a

[41] **Ex. S**.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

consumer's computer. When the consumer attempts to visit an official website, the pharmer's software program redirects the browser to the pharmer's fake version of the website. In this way, the pharmer is able to capture the PII the consumer enters into the counterfeit website, thereby compromising the consumer's account.

58. According to Javelin Strategy and Research, "one in every three people who is notified of being a potential fraud victim becomes one . . . with 46% of consumers who had cards breached becoming fraud victims that same year."[42]

59. Simply reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. The Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 32% spent a month or more resolving problems."[43] In fact, the BJS reported, "resolving the problems caused by identity theft may take more than a year for some victims." *Id*. at 13.

60. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit card accounts were the most common types of misused information. *Id*.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

[42] *Someone Became an Identity Theft Victim Every 2 Seconds Last Year*, Fox Business, Feb. 5, 2014 available at: http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-identitytheft-victim-every-2-seconds-last-year.html (attached hereto as **Exhibit Y**).

[43] *Victims of Identity Theft*, U.S. Department of Justice, September 2015, available at: https://www.bjs.gov/content/pub/pdf/vit14.pdf (attached hereto as **Exhibit Z**).

61. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[44]

F. Annual Monetary Losses from Identity Theft are in the Billions of Dollars

62. Javelin Strategy and Research reports that monetary losses from identity theft increased to $21 billion in 2013.[45] There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[46]

63. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them, and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

---

[44] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), available at: http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (attached hereto as **Exhibit AA**).

[45] *2013 Identity Fraud Report* (attached hereto as **Exhibit AB**)

[46] GAO, *Report to Congressional Requesters*, at 33 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (attached hereto as **Exhibit AC**).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

64. The National Institute of Standards and Technology categorizes the combination of names and credit card numbers as sensitive and warranting a higher impact level based on the potential harm when used in contexts other than their intended use.[47] Private information that is "linked" or "linkable" is also more sensitive. Linked information is information about or related to an individual that is logically associated with other information about the individual. Linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. An example of linking information the NIST report cites is a Massachusetts Institute of Technology study showing that 97% of the names and addresses on a voting list were identifiable using only ZIP code and date of birth.

65. Private information is broader in scope than directly identifiable information. As technology advances, computer programs become increasingly able to scan the Internet with wider scopes to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

G. Plaintiffs and Class Members Suffered Damages

66. The data breach was a direct and proximate result of Brooks Brothers' failure to properly safeguard and protect Plaintiff's and Class Members' Private Identifiable Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Brooks Brothers' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Private

[47] *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology Special Publication 800-122, 3-3, available at: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=904990 (attached hereto as **Exhibit AD**).

Identifiable Information to protect against reasonably foreseeable threats to the security or integrity of such information.

67. Brooks Brothers' itself admits to their shortcomings when it comes to security, as noted in their "Message to Our Customers About Payment Card Security Incident," Brooks Brothers' goes on to state, "[while] we are continuing to review and enhance our security measures moving forward to help prevent a future incident. Again, please accept our sincere regret for any concern that this incident may cause."[48]

68. Plaintiffs' and Class Members' PII is private and sensitive in nature, and it was inadequately protected by Brooks Brothers. Brooks Brothers did not obtain Plaintiffs' and Class Members' consent to disclose their PII except to certain persons not relevant to this action, as required by applicable law and industry standards.

69. As a direct and proximate result of Brooks Brothers' wrongful action and inaction and the resulting data breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

70. Brooks Brothers' wrongful action and inactions directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII, causing them to suffer, and continue to

[48] *Message to Our Customers About Payment Card Security Incident* (attached hereto as **Exhibit AE**).

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Theft of their PII;

b. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class Members' information on the Internet black market;

c. The untimely and inadequate notification of the data breach;

d. The improper disclosure of their PII;

e. Loss of privacy;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

g. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

h. Overpayments to Defendant for purchases during the period of the subject data breach in that implied in the price paid for such product by Plaintiffs and the Class Members to Defendant was the promise that some amount of the product charge would be applied to the costs of implementing reasonable and adequate safeguards and security measures that would protect customers' PII, which Defendant and its affiliates did not implement and, as a result, Plaintiffs and Class Members did not receive what they paid for and were overcharged by Defendant; and

i. Deprivation of rights they possess under the Unfair Competition Laws.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

V. CLASS ACTION ALLEGATIONS

71. Plaintiffs bring this action on their own behalf and pursuant to the Federal Rules of Civil Procedure Rule 23(a), (b)(2), (b)(3), and (c)(4), Plaintiffs seek certification of a Nationwide class and a California class. The nationwide class is initially defined as follows:

> All persons residing in the United States who made purchases at Defendant's stores from the time period of April 14, 2016, and March 1, 2017 (the "Nationwide Class").

The California class is initially defined as follows:

> All persons residing in California who made purchases at Defendant's stores from the time period of April 14, 2016, and March 1, 2017 (the "California Class").

72. Excluded from each of the above Classes are Brooks Brothers, including any entity in which Brooks Brothers has a controlling interest, is a parent or subsidiary, or which is controlled by Brooks Brothers, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Brooks Brothers. Also excluded are the judges and court personnel in this case and any members of their immediate families. Plaintiffs reserve the right to amend the Class definitions if discovery and further investigation reveal that the Class should be expanded or otherwise modified.

73. *Numerosity*. Fed. R. Civ. P. 23(a)(1). The members of the Classes are so numerous that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, Brooks Brothers has acknowledged that customers' Private Identifiable Information was siphoned for a period of almost a year in 223 Brooks Brothers stores. The disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendant's possession, custody, or control.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

74. *Commonality*. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant owed a duty of care to Plaintiffs and Class Members with respect to the security of their personal information;

b. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' personal information;

c. Whether Defendant violated California's Unfair Competition Law by failing to implement reasonable security procedures and practices;

d. Whether Defendant violated common and statutory law by failing to promptly notify Class Members that their PII had been compromised;

e. Which security procedures and which data-breach notification procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;

f. Whether Defendant has an implied contractual obligation to use reasonable security measures;

g. Whether Defendant has complied with any implied contractual obligation to use reasonable security measures;

h. Whether Defendant's acts and omissions described herein give rise to a claim of negligence;

i. Whether Defendant knew or should have known of the security breach prior to its 2017 disclosure;

j. Whether Defendant had a duty to promptly notify Plaintiffs and Class Members that their personal information was, or potentially could be, compromised;

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

k. What security measures, if any, must be implemented by Defendant to comply with its implied contractual obligations;

l. The nature of the relief, including equitable relief, to which Plaintiffs and the Class Members are entitled;

m. Whether Defendant willfully and/or negligently violated the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.*; and

n. Whether Plaintiffs and the Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

75. *Typicality*. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was misused and/or disclosed by Brooks Brothers.

76. *Adequacy of Representation*. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiffs have retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs' claims are typical of the claims of other members of the Classes and Plaintiffs have the same non-conflicting interests as the other Class Members. Therefore, the interests of the Classes will be fairly and adequately represented by Plaintiffs and their counsel.

77. *Superiority of Class Action*. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

78. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment,

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Brooks Brothers' violations of law inflicting substantial damages in the aggregate would go un-remedied.

79. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Brooks Brothers has acted or has refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

VI. CAUSES OF ACTION

COUNT I

Breach of Implied Contract

(On Behalf of Plaintiffs, the Nationwide Class and the California Class)

80. Plaintiffs allege and incorporates herein by reference each and every allegation contained in paragraphs 1 through 79, inclusive, of this Complaint as if set forth fully herein.

81. Brooks Brothers solicited and invited Plaintiffs and the members of the Class to buy its retail merchandise. Plaintiffs and Class Members accepted Brooks Brothers' offers and bought Brooks Brothers' retail merchandise. Implied in Brooks Brothers' offer to sell merchandise was the promise that Plaintiffs' and Class Members' PII would not be harvested by a hacker at the moment of acceptance.

82. When Plaintiffs and Class Members purchased Brooks Brothers' merchandise, they provided their PII. In so doing, Plaintiffs and Class Members entered into implied contracts with Brooks Brothers where Brooks Brothers agreed to safeguard and protect such information, dispose, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised.

83. As noted by Brooks Brothers' itself, "Brooks Brothers values its customers and respects their privacy. We collect customer information in an effort to improve your shopping experience and to communicate with you about

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

our products, services, contests, and promotions. Brooks Brothers recognizes that it must maintain and use customer information responsibly."[49]

84. Each purchase of Brooks Brothers' retail merchandise by Plaintiffs and Class Members was made pursuant to the mutually agreed-upon implied contract with Brooks Brothers under which Brooks Brothers agreed to safeguard and protect Plaintiff's and Class Members' PII and to timely and accurately notify them if such information was compromised or stolen. As stated by Brooks Brothers, "We respect your privacy and, therefore, Brooks Brothers does not sell or rent the personal information you provide to us to any third party you do not wish us to do so."[50]

85. Plaintiffs and Class Members would not have provided and entrusted their PII to Defendant in the absence of the implied contract. As noted by Brooks Brothers' CEO, "[o]ur major asset is our brand . . . [w]e want high expectation customers."[51]

86. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

87. Defendant breached the implied contracts which it made with Plaintiffs and Class Members by failing to safeguard and protect the PII of Plaintiffs and Class Members and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the data breach.

88. Plaintiffs and Class Members have lost the benefit of the bargain by having their PII compromised. Plaintiffs and Class Members have spent more on purchasing Defendant's merchandise than they would have if they had known that Defendant was not providing the reasonable security that Plaintiffs and Class

[49] **Ex. U**.
[50] *Id.*
[51] **Ex. E**.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Members expected. Plaintiffs and Class Members have lost money and/or property as a result of Defendant's actions.

89. Defendant failed to prevent the data breach, which makes Plaintiffs' and Class Members' harm "fairly traceable" to conduct being challenged here.[52]

90. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant and Plaintiffs and Class Members, Plaintiffs and Class Members sustained actual losses and damages in an amount according to proof at trial but in excess of the minimum jurisdictional requirement of this Court.

///

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

[52] As explained by judge Michelle Friedland in *In re Zappos.com, Inc*., 888 F.3d 1020 (9th Cir. 2018):

> That hackers might have stolen Plaintiffs' PII in unrelated breaches, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches (rather than the data stolen from Zappos), is less about standing and more about the merits of causation and damages. As the Seventh Circuit recognized in *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015), that "some other store might [also] have caused the plaintiffs' private information to be exposed does nothing to negate the plaintiffs' standing to sue" for the breach in question.13 Id. at 696; cf. *Price Waterhouse v. Hopkins*, 490 U.S. 228, 263 (1989) (O'Connor, J., concurring in the judgment) ("[I]n multiple causation cases, . . . the common law of torts has long shifted the burden of proof to multiple defendants to prove that their negligent actions were not the 'but-for' cause of the plaintiff's injury." (citing *Summers v. Tice*, 199 P.2d 1, 3–4 (Cal. 1948))), superseded on other grounds by 42 U.S.C. § 2000e-2(m) (2012).

COUNT II

Negligence

(On Behalf of Plaintiffs and the Nationwide and California Classes)

91. Plaintiffs alleges and incorporates herein by reference each and every allegation contained in paragraphs 1 through 90, inclusive, of this Complaint as if set forth fully herein.

92. Upon accepting Plaintiffs' and Class Members' PII in their respective POS systems, Brooks Brothers undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties, and to utilize commercially reasonable methods to do so. This duty included, among other things, designing, maintaining, and testing Brooks Brothers security systems to ensure that Plaintiffs' and the Class Members' PII was adequately secured and protected.

93. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

94. Defendant breached a legal duty independent of any contractual obligation it had to the Plaintiffs and Class Members.

95. Defendant had a duty to Plaintiffs and the Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' PII as required by California Civil Code §1798.81.5 and Federal Trade Commission Act (15 U.S.C. §45). This legal duty arises outside of any contractual, implied or express, responsibilities that Defendant had between Plaintiffs and Class Members, as it is "completely independent" of any contract. *Robinson Helicopter Co., Inc. v. Dana Corp*., 34 Cal.4th 979 (2004).

96. Moreover, had Plaintiffs and Class Members known of Defendant's improper security systems, they would not have entered into an agreement in the

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

first place, and thus, would not have suffered from Defendant's breach of contract itself.

97. Negligence *per se* creates a presumption that affects a cause of action for negligence. Under the doctrine, "the plaintiff 'borrows' statutes to prove duty of care and standard of care." *Johnson v. Honeywell Internat. Inc.*, 179 Cal.App.4th 549 (2009); Evidence Code § 669.

98. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class Members' PII.

99. Defendant breached its duties to Plaintiffs and the Class Members under the Federal Trade Commission Act (15 U.S.C. § 45).

100. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

101. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII in its stores obtained and stored, and the foreseeable consequences of a data breach at a retail chain as large as Defendant's, including, specifically, the damages that would result to Plaintiffs and Class members.

102. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

103. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

104. The harm that occurred as a result of the security breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

105. Defendant also breached its duties to Plaintiffs and Class Members under California Civil Code §1798.81.5 by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class Members' PII. "A business that . . . maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." California Civil Code §1798.81.5 (b) [emphasis added].

106. Plaintiffs and Class members are within the class of persons that California Civil §1798.81 is meant to protect. "It is the intent of the Legislature to ensure that personal information about California residents is protected." California Civil Code §1798.81.5 (a)(1).

107. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*, which creates a presumption of negligence. *Das v. Bank of Am., N.A.*, 186 Cal. App. 4th 727, 737 (2010).

108. But for Defendant's negligence *per se*, Plaintiffs and the Class Members would not have been harmed.

109. The injury and harm suffered by Plaintiffs and the Class Members was the reasonably foreseeable result of Defendant's negligence *per se*.

110. Defendant knew or should have known that its negligence *per se* would cause Plaintiffs and the Class Members to experience the foreseeable harms associated with the exposure of their PII.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

111. A "special relationship" exists between Defendant and the Plaintiffs and Class Members. Defendant entered into a "special relationship" with the Plaintiffs and Class Members whose PII was solicited, requested, collected - with every purchase - and received by Defendant. Defendant entered into a "special relationship" with all Plaintiffs and Class Members by placing their PII in their database, sharing with its affiliates, and using this information to target specific marketing efforts to Plaintiffs and Class Members, as noted by Defendant, "We collect customer information in an effort to improve your shopping experience and to communicate with you about our products, services, contests, and promotions. Brooks Brothers recognizes that it must maintain and use customer information responsibly."[53] Furthermore, Defendant also created a "special relationship" with Plaintiffs and Class Members who provided their information to Defendant and its affiliates, by playing a large role in creating and maintaining centralized computer systems and data security practices that were used for storage of all of Defendant's customers' PII.[54] Finally, Defendant also created a "special relationship" with Plaintiffs and Class Members whose PII was placed in the Defendant database due to their dealings with its affiliated companies, as stated by Brooks Brothers, "Brooks Brothers may share information with its subsidiaries and other affiliated companies, and with other carefully selected vendors and business partners with whom we work. This includes companies that perform fraud prevention/detection services; assist us in providing our products and services to you; assist in maintaining and managing customer information to provide customer and internet services; take and fulfill orders; conduct Brooks Brothers promotions and surveys; or assist us in more effectively communicating with our customers. All companies that act on our behalf are contractually obligated to keep all information confidential and to use the customer information only to provide the services we

[53] **Ex. U**.
[54] *See* **Ex. U** and **V**.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

ask them to perform for you and us."[55] Plaintiffs' and Class Members' PII was placed in the Defendant's and/or its affiliates' database so that they tailor their marketing efforts to Plaintiffs and Class Members.

112. In addition, due to Defendant's negligence, Plaintiffs and Class Members have suffered a loss of value in the form of diminution in the value of their PII. The diminution in the value of Plaintiffs and Class Members' PII results in physical damage to their property, namely, their PII.

113. Defendant had a duty to timely disclose to Plaintiffs and Class Members that their PII had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiffs and Class Members could take appropriate measures to avoid use of bank funds and monitor their account information and credit reports for fraudulent activity.

114. Defendant breached its duty to discover and to notify Plaintiffs and Class Members of the unauthorized access by failing to discover the security breach within reasonable time and by failing to notify Plaintiffs and Class Members of the breach until May 2017. To date, Defendant has not provided sufficient information to Plaintiffs and Class Members regarding the extent and scope of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

115. Defendant also breached its duty to Plaintiffs and Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering its negligent practices, Defendant failed to provide adequate supervision and oversight of the PII, in spite of the known risk and foreseeable likelihood of breach and misuse,

[55] **Ex. U**.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

which permitted a third party to gather Plaintiffs' and Class Members' PII, misuse the PII, and intentionally disclose it to others without consent.

116. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs and Class Members' PII during the time it was within Defendant's control.

117. Through Defendant's acts and omissions as described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendant unlawfully breached its duty to exercise reasonable care to adequately protect and secure Plaintiffs' and Class Members' PII during the time it was within Defendant's control.

118. Further, through its failure to timely discover and provide clear notification of the data breach to consumers, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII.

119. Upon information and belief, Defendant improperly and inadequately safeguarded the PII of Plaintiffs and Class Members and did so in a manner that deviated from standard industry rules, regulations, and practices at the time of the data breach.

120. Defendant's failure to take proper security measures to protect Plaintiffs' and Class Members' sensitive PII, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' PII.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

121. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct adequate regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class Members' PII.

122. Neither Plaintiffs nor the other Class Members contributed to the data breach and subsequent misuse of their PII as described in this Complaint.

123. Defendant failed to prevent the data breach, which makes Plaintiffs' and Class Members' harm "fairly traceable" to conduct being challenged here.[56]

124. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members sustained actual losses and damages in an amount according to proof at trial but in excess of the minimum jurisdictional requirement of this Court.

COUNT III

Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code § 17200 Unlawful Business Practices

(On Behalf of Plaintiffs and the California Class)

125. Plaintiffs allege and incorporates herein by reference each and every allegation contained in paragraphs 1 through 124, inclusive, of this Complaint as if set forth fully herein.

126. Defendant has violated Cal. Bus. and Prof. Code §17200 et seq. by engaging in unlawful, unfair or fraudulent business acts and practices that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code §17200.

127. Defendant violated Cal. Civ. Code Section 1798.81, which requires that "[a] business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal

[56] *Id.*

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means." Defendant violated Section 1798.81 by failing to erase or modify personal information, e.g. full names, credit card numbers, credit card verification codes, and zip codes, in its records of sales of goods to Plaintiffs. Instead, Defendant maintained its records in an unsecured electronic environment that left personal information susceptible to unauthorized access. Had the Defendant erased or modified the Plaintiffs' personal information, third-party hackers would not have been able to obtain Plaintiffs' full names, credit card numbers, credit card verification codes, and zip codes.

128. As a direct and proximate result of Defendant's unlawful acts and practices, Plaintiffs and the Class Members were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

129. Defendant also violated Cal. Civ. Code Section 1798.81.5(b), which states in relevant part, that a business that "maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure…." Personal information under the statute is "[a]n individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted" with "[a]ccount number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Cal. Civ. Code Section 1798.81.5(d)(1)(A)(iii). Defendant violated Section 1798.81.5(b) by maintaining Plaintiffs' and Class Members' PII in an unsecure

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

electronic environment, and even when Defendant discovered the full scope of unauthorized access of Plaintiffs' and Class Members' PII and Defendant failed to notify Plaintiffs for approximately eight (8) months. Had the Defendant maintained the Plaintiffs' personal information, third-party hackers would not have been able to obtain Plaintiffs' full names, credit card numbers, credit card verification codes, and zip codes.

130. As a direct and proximate result of Defendant's unlawful acts and practices, Plaintiffs and the Class Members were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

131. In addition, Defendant engaged in unlawful acts and practices with respect to its services by failing to discover and then disclose the data breach to Plaintiffs and Class Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82(a), which requires that a "business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or useable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

the breach and restore the reasonable integrity of the data system." Defendant was in violation of this statute because it unnecessarily delayed disclosure to Plaintiffs of the data breach subject to this action. It still is in violation of this statute by failing to provide disclosure to Plaintiffs in a manner where they would reasonably see it.

132. To date, Defendant still has not provided sufficient information to Plaintiffs and the Class Members.

133. Plaintiffs and the Class Members seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq*., including, but not limited to, restitution to Plaintiffs and Class Members of money or property that Defendant acquired from Plaintiffs and the Class Members by means of its unlawful, and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT IV

Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code §17200 Unfair Business Practices

(On Behalf of Plaintiffs and the California Class)

134. Plaintiffs alleges and incorporates herein by reference each and every allegation contained in paragraphs 1 through 133, inclusive, of this Complaint as if set forth fully herein.

135. Defendant engaged in unfair acts and practices by soliciting and collecting Plaintiffs' and Class Members' PII with knowledge that the information would not be adequately protected while Plaintiffs' and the Class Members' PII would be processed in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Class Members. They were likely to deceive the public into believing their PII was secure, when it was not. The

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

harm these practices caused to Plaintiffs and Class Members outweighed their utility, if any.

136. Defendant engaged in unfair acts and practices with respect to the provision of its services by failing to enact adequate privacy and security measures to protect Plaintiff's and Class Members' PII from further unauthorized disclosure, release, data breaches, and theft and by failing to timely discover and give notice of the data breach. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Class Members. They were likely to deceive the public into believing their Private Identifiable Information was secure, when it was not. The harm these practices caused to Plaintiffs and the Class Members outweighed their utility, if any.

137. As a direct and proximate result of Defendant's unfair practices and acts, Plaintiff and the Class Members were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

138. Plaintiffs and the Class Members seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq*., including, but not limited to, restitution to Plaintiffs and Class Members of money or property that Defendant acquired from Plaintiffs and the Class Members by means of its unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

///

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

COUNT V

Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code §17200 Fraudulent/Deceptive Business Practices

(On Behalf of Plaintiffs and the California Class)

139. Plaintiffs allege and incorporate herein by reference each and every allegation contained in paragraphs 1 through 138, inclusive, of this Complaint as if set forth fully herein.

140. Defendant engaged in fraudulent and deceptive acts and practices by omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' PII. Defendant effectively concealed the inadequate security of Plaintiffs' personal information and the resultant data breach by embedding notice of the breach in a remote part of the Defendant's website.

141. As a direct and proximate result of Defendant's deceptive practices and acts, Plaintiffs and the Class Members were injured and lost money or property, including but not limited to the loss of their legally protected interest in the confidentiality and privacy of their PII, and additional losses described above.

141. Plaintiffs and the Class Members seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq*., including, but not limited to, restitution to the Plaintiffs and Class Members of money or property that Defendant acquired from Plaintiffs and the Class Members by means of its fraudulent and deceptive business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

///

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

COUNT VI

Breach of the Covenant of Good Faith and Fair Dealing

(On Behalf of Plaintiffs, the Nationwide Class and the California Class)

142. Plaintiffs alleges and incorporates herein by reference each and every allegation contained in paragraphs 1 through 141, inclusive, of this Complaint as if set forth fully herein.

143. The law implies a covenant of good faith and fair dealing in every contract.

144. Plaintiffs and Class Members contracted with Defendant by accepting Defendant's offers and paying for products at Defendant's stores.

145. Plaintiffs and Class Members performed all of their duties under their agreements with Defendant.

146. All of the conditions required for Defendant's performance under the contract have occurred.

147. Defendant did not provide and/or unfairly interfered with and/or frustrated the right of Plaintiffs and the Class Members to receive the full benefits under their agreements.

148. Defendant breached the covenant of good faith and fair dealing implied in its contracts with Plaintiffs and the Class Members by failing to use and provide reasonable and industry-leading security practices to safeguard the PII of Plaintiffs and the Class Members.

149. Plaintiffs and the Class Members were damaged by Defendant's breach in that they paid for, but never received, the valuable security protections to which they were entitled.

150. As a direct and proximate result of Defendant's breach of the covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

COUNT VII

Violation of California Data Breach Act

(On Behalf of Plaintiffs and the California Class)

151. Plaintiffs allege and incorporate herein by reference each and every allegation contained in paragraphs 1 through 150, inclusive, of this Complaint as if set forth fully herein.

152. Defendant was required, but failed, to take all reasonable steps to dispose, or arrange for the disposal, of records within its custody or control containing PII when the records were no longer to be retained, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

153. Defendant's conduct, as alleged herein above, violated California, Cal. Civ. Code §§ 1798.80 *et. seq.*

154. Defendant was required, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.

155. The data breach constituted a "breach of the security system" within the meaning of section 1798.82(g) of the California Civil Code.

156. The information compromised in the data breach constituted "personal information" within the meaning of section 1798.80(e) of the California Civil Code.

157. California Civil Code § 1798.80(e) requires disclosure of data breaches "in the most expedient time possible and without unreasonable delay…."

158. Defendant violated Cal. Civ. Code § 1798.80(e) by unreasonably delaying disclosure of the data breach to Plaintiffs and other Class Members, whose PII was, or was reasonably believed to have been, acquired by an unauthorized person.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

159. Upon information and belief, no law enforcement agency instructed Defendant that notification to Plaintiffs and Class Members would impede a criminal investigation.

160. As a direct and proximate result of Defendant's violation of Cal. Civ. Code § 1798.80, *et seq*., Plaintiffs and Class Members incurred economic damages, including expenses associated with monitoring their personal and financial information to prevent further fraud.

161. Plaintiffs and the Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) actual damages suffered by Class Members as alleged above; (b) statutory damages for Defendant's willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; (c) equitable relief; and (d) reasonable attorneys' fees and costs under Cal. Civ. Code §1798.84(g).

162. In violating the California Data Breach Act, Defendant acted in a willful, wanton and malicious manner, in callous and conscious disregard for the rights and interests of Plaintiffs and the Class Members, and with knowledge that its conduct would substantially annoy, vex and damage Plaintiffs and the Class Members thereby entitling Plaintiffs and the Class Members to recover punitive and exemplary damages against Defendant pursuant to California Civil Code section 3294 in an amount according to proof at trial.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members, respectfully requests that the Court enter judgment in his favor and against Defendant as follows:

A. For an Order certifying the Nationwide Class and California Class as defined here, and appointing Plaintiffs and his Counsel to represent the Nationwide Class and the California Class;

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Brooks Brothers to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of PII compromised;

D. For restitution and disgorgement of the revenues wrongfully obtained as a result of Defendant's wrongful conduct;

E. For an award of actual damages and compensatory damages, in an amount to be determined at trial;

F. For punitive and exemplary damages;

G. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and

H. For such other and further relief as this Court may deem just and proper.

///

///

///

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

VIII. DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: June 28, 2018

Respectfully Submitted,

/s/ *Bobby Saadian*
Bobby Saadian
Attorneys for Plaintiffs

/s/ *Thomas V. Girardi*
Thomas V. Girardi
Attorneys for Plaintiffs

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137